ISSN:0975-9646

Forensic-as-a-Service for Mobile Devices (Literature Survey)

Prashant N. Ninawe[1]
Department of Computer Technology
YCCE, Nagpur-441110, Maharashtra, India

Prof. Shrikant B. Ardhapurkar[2]
Department of Computer Technology
YCCE, Nagpur-441110, Maharashtra, India

Abstract- **Cloud computing is a relatively new concept that offers the potential to deliver scalable elastic services to many. The notion of pay-per use is attractive and in the current global recession hit economy it offers an economic solution to an organization's IT need. Computer forensic is a relatively new discipline born out of the increasing use of computing and digital storage devices in criminal acts (both traditional and hi-tech). As per the survey of BI Intelligence there are 1.4 billion Smartphone in use by December 2013. With the increased availability of these powerful devices, there is also a potential increase for criminals to use this technology as well. Criminals could use smart phones for number of activities such as committing fraud over e-mail, harassment through text messages, communications related to narcotics etc. The data stored on smart phones could be extremely useful to analysts through the course of an investigation. Indeed mobile devices are already showing themselves to have a larger volume to probative information that is link to an individual with just basic call history, contact and text message data; smart phone contains even more useful information, such as e-mail, browser history and chat logs. Mobile devices probably have more probative information that can be linked to an individual per byte examined than most computers and this data is harder to acquire in a forensically proper fashion. This paper describes technical problems and challenges encountered in cloud for android mobile forensics.**

Keywords- **cloud computing, digital forensic, mobile device forensic, cloud forensic, forensic challenges**

I. INTRODUCTION

The cloud computing is a very popular topic in recent year. It includes the following key characteristic: agility, low cost in using device and location independence, virtualization, reliability, scalability and elasticity, performance and etc. All those features show fascinating benefit to companies. As they can get free from the worry about the investment on hardware and can setup up their business easily. There are three major type of cloud services delivery model: Infrastructure as a service (IaaS), Platform as a service (PaaS), and Software as a service (SaaS). Different type of delivery model provides different convenience. IaaS just like server-hosting services, but consumer do not need pay-for-hardware and maintain them anymore. They benefit much form the scalability and elasticity. PaaS is like service hosting, but consumers do not need to worry about the server out of working or not able to response to large number of request. They benefit much form the performance and reliability. SaaS look like the Representational State Transfer (REST) very much, and make consumers benefit from performance, multi-tenancy architecture and many other features.

But two of the three models is share a weakness from the characteristics of the cloud computing. As consumer put their logical procedurals on the cloud, which mean that they do not own the control of the hardware specially for PaaS and SaaS. This is not friendly to digital forensic. Because traditional digital forensic is deeply depending on the media seized from the crime scene. At this point, there should be changes or enhancement for cloud computing to be friendlier with digital forensics.

II. CLOUD COMPUTING

Cloud computing as Fig. 1 makes a virtual pool of resources such as storage, CPU, network and memory too fulfill the user's resource requirement and provides on demand (Pay per use) hardware and software without barriers. It can be named as dynamic computing because it provides resources when required (dynamically). Cloud computing manages the pool of resources automatically and dynamically through software and hardware [1].

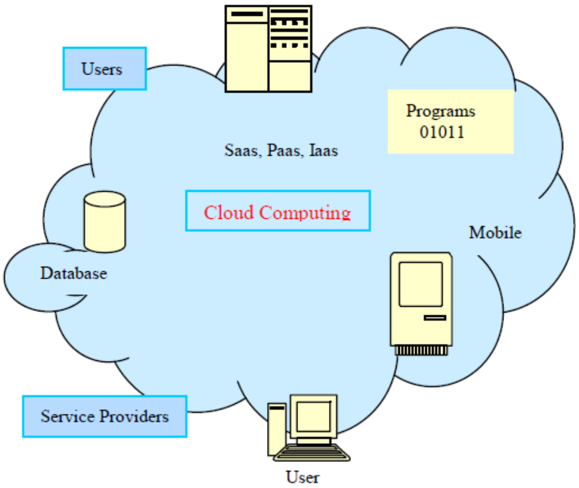

Fig. 1 Cloud Computing Model

There are mainly three types of Cloud Computing model, *Private Cloud, Public Cloud* and *Hybrid Cloud*:

i. *Private Cloud:* It is a proprietary architecture subscribed by an organization, which provides hosted services to the users within the organization. This is protected by the firewall to form barrier against outside the world to access hosted services from the private cloud.\

ii. *Public Cloud:* It is not proprietary of any organization; the services provided in this clouds can be accessed by any organization.

iii. *Hybrid Cloud:* In hybrid cloud, the services are offered to the limited and well defined number of parties.

It can make internet as a desktop. As we work on desktop, cloud computing can be used in the same manner. Many organizations have started implementing cloud computing like Amazon, Google and Microsoft etc.

In cloud computing, various service providers participate to provide services like storage, network, CPU, hardware and software etc. if user doesn't have storage on personal computers, he can use cloud computing to take advantage of cloud's storage to store his documents without worrying. Same type of service is provided by Flickr.com which can be used to upload image on Flickr's server. User can use it as he is working on his desktop but he requires internet when images are to process on desktop. GoogleApps is used to create document online. Such type of services are available in the cloud computing. Cloud computing is not limited to specific data centers while it can use many data centers distributed in various geographical location. Cloud computing can be implemented in mainly three styles.

A. *Software-as-a-Service (SaaS):* Software service provider provides software in the cloud. Users can use these services as software and do his work without installing the same in the local system. GoogleApps provides such services to create documents and spreadsheets online without installing any document or spreadsheet application in his local system.

B. *Platform-as-a-Service (PaaS):* Platform as a service allows user to use cloud computing for developing or executing any application using development kit provided by cloud computing. User are not required to installed development kit on local system, he can use installed software or development kit in cloud computing to develop any program or application. Mainly Oracle involves in providing Platform-as-a-Service.

C. *Infrastructure-as-a-Service (IaaS):* Infrastructure as a service provide us a feature to install and execute the software. Here, user can gain access to virtualized server. IaaS targets operating system, hardware, CPUs and embedded system, network and storage. This enables a homogeneous virtualized environment where specific software will be installed and executed. Mainly Amazon involves in providing Infrastructure-as-a-Service.

III. MOBILE FORENSICS

Mobile Forensics is defined as the science of recovering digital evidence from a mobile phone under forensically sound conditions using acceptable methods [2]. The process of Mobile Forensic has four steps Data Preservation, Data Acquisition, Data Examination and Analysis and final step in the Mobile Forensic is the Reporting.

A. *Data Preservation:* The very first step in the Mobile Forensic is the data preservation step in digital evidence recovery and it is the process of seizing and securing suspected evidence without deleting or modifying the actual data that is present in the mobile devices.

B. *Data Acquisition:* After successful preservation of the data the second step of the Mobile Forensic is the data Acquisition step. Acquisition is the process or method of imaging or otherwise obtaining information from digital evidence and its peripheral equipment and media. There are four types of data Acquisition methods are available they are as follows: Manual Acquisition, Logical Acquisition, Physical Acquisition and Chip-off [3]. All these methods are used for acquiring the internal and external memory data from the mobile phones.

C. *Data Examination and Analysis:* Data Examination and Analysis is the process of applying tools to uncover digital evidence including that which may be hidden, deleted or obscured.

D. *Reporting:* This stage is most important. Everything done during the mobile forensics is useless if the evidence is not admitted correctly in the court to prove or defend the possible crime. The authenticity of evidences must ensure by a well documented regarding of possessing the evidences from the start of the forensic process to the end of the process when all evidences admitted in the court.

IV. FORENSICS-AS-A-SERVICE

When Forensics comes to the Cloud Computing services, we could have to understand the two perspective: one is to regard it as an object to be investigated and the other is trying to utilize it for investigative analysis [4]. Up to the date the maximum of studies have been focused on the first one which considers the cloud computing service as one of the major forensically investigated targets. There are few more studies using the cloud computing service for improving the investigation performance or convenience. Instead some researchers have used the distributed computing system which could give similar effect as the Cloud Computing service does.

V. CHALLENGES OF FORENSIC INVESTIGATION IN CLOUD COMPUTING

Digital investigations are about control of forensic evidence data. From the technical standpoint, this data can be available in three different states: at rest, in motion or in execution [5]. Data at rest means that the data is static and is present in the storage media or disk space. Data in motion represents the data is transferred from one entity to another entity by using network connection or by using internet. In third state the data is loaded into the program memory and executed as a process. In this case the data is neither at rest or in motion but the data is present in the execution step.

Traditional mobile forensic methodologies allow investigators to seize equipment and perform analysis on the media and data recovered. In a distributed infrastructure organization, investigators are confronted with an entirely different situation. They have no longer the option of seizing physical data storage on Cloud Environment. Data and processes of the customer are dispensed over an undisclosed amount of virtual instances, applications and network elements. Hence, there is a problem whether preliminary findings of the mobile forensic community in the field of digital forensics apparently have to be revised and adapted to the new environment.

Within this section, we discuss the issues of investigations in SaaS, PaaS and IaaS environments.

A. *SaaS Environment:* In the SaaS model, the customer or the user does not have permission to obtain any control of the underlying operating infrastructure such as network, servers, operating systems or the application that is used. It means that no deeper view into the system and its underlying infrastructure is provided to the customer. Only limited user- specific application configuration settings can be controlled contributing to the evidences which can be extracted from the client.

B. *PaaS Environment:* The main advantages of the PaaS model is that the developed software application is under the control of the customer and except for some Cloud Service Provider, the source code of the application does not have to leave the local development environment. Given these circumstances, the customer obtains theoretically the power to dictate how the application interacts with other entities such as databases, storage, network etc. Cloud Service Provider normally claim this transfer is encrypted but this statement can hardly be verified by the customer. Since the customer has the ability to interact with the platform over a prepared API, system states and specific application logs can be extracted.

C. *IaaS Environment:* As expected, even virtual instances in the cloud get compromised by adversaries. Hence, the ability to determine how protection in the virtual environment failed and to what extent the affected systems have been compromised is very harmful not only for recovering from an incident or a mobile devices. Also forensic investigations gain advantage from such information and contribute to resilience against future attacks on the systems.

VI. CONCLUSION

Forensic technology under the cloud computing is a new subject for the computer forensic workers. Currently there is still no authoritative technology standard, so a large quantity of things is waiting to be done. This paper we preliminarily discussion about cloud computing, mobile forensic and the challenges of mobile forensic under Cloud Computing environment, The purpose is to serve as the modest spur, hoping that more and more people will concentrate on it and devote to it.

REFERENCES

[1] Rajan S, Jairath A, “Cloud Computing: The Fifth Generation of Computing”, Communication Systems and Network Technologies (CSNT), 2011 International Conference on , 3-5 June 2011,pp 665 - 667

[2] Raghav S, Saxena A.K, “Mobile forensics: Guidelines and challenges in data preservation and acquisition”, Research and Development (SCOReD), 2009 IEEE Student Conference on, 16-18 Nov. 2009,pp 5 - 8

[3] Alghafli, K.A., Jones, A., Martin, T.A., “Forensics data acquisition methods for mobile phones”, Internet Technology And Secured Transactions, 2012 International Conference for , 10-12 Dec. 2012, pp 265 – 269

[4] Jooyoung Lee, Sungyong Un, “Digital forensics as a service: A case study of forensic indexed search”, ICT Convergence (ICTC), 2012 International Conference on, 15-17 Oct. 2012, pp 499 – 503

[5] Birk D, Wegener C, “Technical Issues of Forensic Investigations in Cloud Computing Environments ” Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop on, 26-26 May 2011, pp 1 - 10